

THE HONORABLE TANA LIN

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

JACQ NIENABER, on behalf of herself and
all others similarly situated,

Plaintiff,

v.

OVERLAKE HOSPITAL MEDICAL
CENTER,

Defendant.

No. 2:23-cv-01159-TL

**PLAINTIFF'S MEMORANDUM IN
OPPOSITION TO DEFENDANT
OVERLAKE HOSPITAL MEDICAL
CENTER'S MOTION TO DISMISS
UNDER RULE 12(B)(6)**

NOTE ON MOTION CALENDAR:
NOVEMBER 20, 2023

WITH ORAL ARGUMENT

TABLE OF CONTENTS

I.	INTRODUCTION	1
II.	FACTUAL BACKGROUND.....	3
III.	LEGAL STANDARD.....	4
IV.	ARGUMENT.....	5
A.	The Complaint Alleges More Than “Tracking” Of “Public Website Browsing Activity”.....	5
B.	Plaintiff Properly Pleads A Claim For Negligence.....	6
C.	Plaintiff Has Adequately Pled An Invasion Of Privacy Claim.....	9
D.	Plaintiff States a Breach of Confidence Claim	11
E.	Plaintiff Adequately States a Breach of Implied Contract Claim	12
F.	Plaintiff Adequately States an Unjust Enrichment Claim.....	14
G.	Plaintiff’s Claims Under the Electronic Communications Privacy Act (“ECPA”) (Counts VI-VIII) are Well Plead.	16
1.	Plaintiff Appropriately Invokes the Tortious or Criminal Conduct Exception to the One-Party Consent Rule.	16
2.	Plaintiff’s Allegations Clearly and Adequately Set Forth Her Claims Under the ECPA.	17
3.	Defendant Provides an Electronic Communication Service and is Subject to the ECPA and the Stored Communication Act (“SCA”).....	20
H.	Plaintiff Adequately Alleges a Claim under the CFAA for Defendant’s Unauthorized Access of Plaintiff’s Computer under False Pretenses	21
I.	Plaintiff Has Sufficiently Pled A Claim Under The Washington Consumer Protection Act.	23
V.	CONCLUSION.....	25

TABLE OF AUTHORITIES

Cases

<i>Affiliated FM Ins. Co. v. LTK Consulting Servs., Inc.</i> , 243 P.3d 521, 526 (Wash. 2010).....	9
<i>America Online, Inc. v. LCGM, Inc.</i> , 46 F.Supp.2d 444 (E.D. Va., 1998).....	22
<i>Armijio v. Yakima HMA, LLC</i> No. 11-CV-3114-TOR, 2012 WL 25766424 (E.D. Wash. July 3, 2012)	9
<i>Bailie Commc'ns, Ltd v. Trend Bus. Sys., Inc.</i> , 810 P.2d 12 (Wash. App. 1991).....	14
<i>Bell Atl. Corp. v. Twombly., (Google RTB II)</i> 550 U.S. 544, 570 (2007) (“Google RTB II”).....	4, 6, 19
<i>Berger v. Sonneland</i> , 144 Wash. 2d 91, 106 (2001)	11, 12
<i>Brown v. Google LLC</i> , No. 20-CV-03664-LHK, 2021 WL 6064009 (N.D. Cal. Dec. 22, 2021).....	24
<i>Brown v. Google LLC</i> , No. 4:20-CV-3664-YGR, 2023 WL 5029899 (N.D. Cal. Aug 7, 2023).....	5
<i>Buckley v. Santander Consumer USA, Inc.</i> , No. C17-5813 BHS, 2018 WL 1532671 (W.D. Wash. Mar. 29, 2018).....	8
<i>Clark v. TRC Env't Corp.</i> , No. C09-1854-JCC, 2011 WL 3664884 (W.D. Wash. Aug. 19, 2011)	7
<i>Cousins v. Sharp Healthcare</i> 22-CV-2040-MMA (DDL), 2023 WL 4484441 (S.D. Cal. July 12, 2023)	5
<i>Cyr v. Orlando Health</i> , No. 8:23-cv-588, ECF No. 37 (M.D. Fl. July 5, 2023)	6
<i>Doe v. Bon Secours Mercy Health</i> , No. A2002663, 2021 WL 9939010 (Ohio Com.Pl. Nov. 22, 2021).	2, 5
<i>Doe v. Boone Health, Inc.</i> , No. 22AC-CC07646, 2023 WL 4996117 (Mo. Cir. July 20, 2023);	2, 6, 13, 15
<i>Doe v. Meta Platforms, Inc.</i> , No. 22-cv-03580-WHO, 2023 WL 5837443 (N.D. Cal. Sept. 7, 2023)	<i>passim</i>
<i>Doe v. Regents of Univ. of California</i> , No. 23-CV-00598-WHO, 2023 WL 3316766 (N.D. Cal. May 8, 2023);	2, 5, 13
<i>Ehling v. Monmouth-Ocean Hosp. Serv. Corp.</i> , 961 F. Supp. 2d 659, 667 (D. N.J. 2013)	20

1	<i>Facebook Internet Tracking Litig.,</i>	
2	140 F. Supp. 3d 922 (N.D. Cal. 2015)	19
3	<i>Feins v. Goldwater Bank NA,</i>	
4	No. CV-22-00932-PHX-JJT, 2022 WL 17552440 (D. Ariz. Dec. 9, 2022)	9
5	<i>Flores-Mendez v. Zoosk, Inc.</i>	
6	No. C 20-04929 WHA, 2021 WL 308543 (N.D. Cal. Jan 30, 2021)	9
7	<i>Guy v. Convergent Outsourcing, Inc.,</i>	
8	No. C22-1558 MJP, 2023 WL 4637318 (W.D. Wash. July 20, 2023).	11, 24
9	<i>Hankins v. City of Tacoma,</i>	
10	No. C06-5099 FDB, 2007 WL 208419, at *2 (W.D. Wash. Jan. 24, 2007)	6
11	<i>Heeger v. Facebook, Inc.,</i>	
12	509 F. Supp. 3d 1182, 1191 (N.D. Cal. 2020)	16
13	<i>I.M.S. Inquiry Mgmt. Sys., Ltd. v. Berkshire Info. Sys., Inc.,</i>	
14	307 F. Supp. 2d 521, 525 (S.D.N.Y. 2004)	23
15	<i>In re Carrier IQ, Inc.,</i>	
16	78 F. Supp. 3d 1051 (N.D. Cal. 2015).	18
17	<i>In re Experian Data Breach Litig.,</i>	
18	No. SACV-15-1592 AG (DFMx), 2016 WL 7973595 (C.D. Cal. Dec. 29, 2016)	14
19	<i>In re Facebook Privacy Litig.,</i>	
20	573 F. App'x 494 (9th Cir. 2014)	14
21	<i>In re Google Cookie Placement Consumer Priv. Litig.,</i>	
22	806 F.3d 125, 145 (3rd Cir. 2015)	17
23	<i>In re Google RTB Consumer Priv. Litig.,</i>	
24	606 F. Supp. 3d 935, 942 (N.D. Cal. 2022)	4
25	<i>In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig.,</i>	
26	440 F. Supp. 3d 447 (D. Md. 2020)	9, 13
27	<i>In re MCG Health Data Sec. Issue Litig.,</i>	
	No. 2:22-CV-849-RSM-DWC, 2023 WL 3057428 (W.D. Was. Mar. 27, 2023)	7
	<i>In re Mednax Servs., Inc., Customer Data Sec. Breach Litig.,</i>	
	603 F. Supp. 3d 1183 (S.D. Fla. 2022)	14, 24
	<i>In re Meta Pixel Healthcare Litig.,</i>	
	No. 22-cv-03580-WHO, 2022 WL 17869218 (N.D. Cal. Dec 22, 2022)	10, 19
	<i>In re Pharmatrak, Inc.</i>	
	329 F.3d 9. 12 (1 st Cir. 2003)	6
	<i>In re Toys R Us, Inc., Privacy Litig.,</i>	
	No. 00-cv-2746, 2001 WL 34517252, at *10-11 (N.D. Cal. Oct. 9, 2001)	23

1	<i>In re Zynga Priv. Litig.</i>	
2	750 F.3d 1098 (9th Cir. 2014).....	19
3	<i>Javier v. Assurance IQ, LLC,</i>	
4	2022 WL 1744107 (9th Cir. May 31, 2022)	6
5	<i>Johnson v. Nasi,</i>	
6	50 Wn. 2d 87, 91, 309 P.2d 380, 383 (1957)).	12
7	<i>Katz-Lacabe v. Oracle Am., Inc.,</i>	
8	No. 22-cv-04792-RS, 2023 WL 2838118 (N.D. Cal. Apr. 6, 2023).....	10
9	<i>Klein v. Facebook, Inc.,</i>	
10	580 F. Supp. 3d 743 (N.D. Cal. 2022)	14, 24
11	<i>Klem v. Wash. Mut. Bank,</i>	
12	295 P.3d 1179, 1187 (Wash. 2013).....	23
13	<i>Kurowski v. Rush Sys. for Health,</i>	
14	No. 22 C 5380, 2023 WL 2349606 (N.D. Ill. Mar. 3, 2023)	11, 21
15	<i>Lopez v. Smith,</i>	
16	203 F.3d 1122, 1127 (9th Cir. 2000)).	5
17	<i>Murphy v. Thomas Jefferson Univ. Hosps., Inc.,</i>	
18	No. CV 22-4674, 2023 WL 7017734, at *4 (E.D. Pa. Oct. 10, 2023)	8
19	<i>Norman-Bloodsaw v. Lawrence Berkeley Lab’y,</i>	
20	135 F.3d 1260 (9th Cir. 1998)	10
21	<i>Opris v. Sincera Reprod. Med.,</i>	
22	No. CV 21-3072, 2022 WL 1639417 (E.D. Pa. May 24, 2022)	8
23	<i>Panag v. Farmers Ins. Co. of Wash.,</i>	
24	204 P.3d 885, 889 (Wash. 2009).....	23
25	<i>Rex v. Chase Home Fin. LLC,</i>	
26	905 F. Supp. 2d 1111 (C.D. Cal. 2012).....	24
27	<i>Rodriguez v. Google LLC,</i>	
	No. 20-cv-04688-RS, 2021 WL 2026726 (N.D. Cal. May 21, 2021).	10
	<i>Smallman v. MGM Resorts Int’l,</i>	
	638 F. Supp. 3d 1175 (D. Nev. 2022)	9, 14, 24
	<i>Smith v. Driscoll,</i>	
	94 Wash. 441, 162 P. 572 (1917)	12
	<i>Smith v. Facebook</i>	
	262 F. Supp. 3d 943 (N.D. Cal. 2017)	5
	<i>Stake v. Knox Community Hosp.,</i>	
	No. 23OT01-0026, 2023 WL 5719594 (Ohio Com.Pl. Aug. 24, 2023);	2, 6

1	<i>Van Buren v. United States</i> ,	
2	141 S.Ct. 1648 (2021)	22
3	<i>Veridian Credit Union v. Eddie Bauer, LLC</i> ,	
4	295 F. Supp. 3d 1140 (W.D. Wash. 2017).....	<i>passim</i>
5	<i>Wesch v. Yodlee, Inc.</i> ,	
6	No. 20-CV-05991-SK, 2021 WL 6206644 (N.D. Cal. July 19, 2021)	20
7	<i>Yockey v. Salesforce, Inc.</i>	
8	No. 22-cv-09067-JST, 2023 WL 5519323 (N.D. Cal. Aug 25, 2023).....	6
9	<i>Young v. Young</i> ,	
10	164 Wash. 2d 477, 191 P.3d 1258 (2008).	12, 14
11	Statutes	
12	Wash Rev. Code 70.02.170.....	6
13	Wash Rev. Code § 19.86.020.....	23
14	18 U.S.C. § 2510.....	19
15	18 U.S.C. § 2511.....	17
16	Wash Rev. Code 70.02.20.....	6
17	Wash Rev. Code 70.02.50.....	6
18	18 U.S.C. §§ 1030.....	21, 22, 23
19	Other Authorities	
20	Restatement (Second) of Torts § 286.....	7

I. INTRODUCTION

Using hidden tracking tools embedded on its website, <https://www.overlakehospital.org>, (the “Website”), Defendant Overlake Hospital Medical Center (“Overlake” or “Defendant”) surreptitiously forced Plaintiff’s and Class Members’ web browsers to send their confidential and highly sensitive personally identifiable information (“PII”) and personal health information (“PHI”) (collectively, “Private Information”) to undisclosed third parties such as Meta Platforms, Inc. (“Facebook”) without Plaintiff’s or Class Members’ knowledge or consent. Defendant’s Website allows those third parties to intercept Plaintiff’s and Class Members’ communications, including booking of appointments, searches for specific medical treatment, particular health conditions, and other sensitive information. These are not “commonly used web-browsing analytics technologies” – they are bugs planted on Plaintiff’s and Class Members’ web browsers for the specific purpose of intercepting, recording, and disclosing Plaintiff’s and Class Members’ communications with Defendant so Defendant can barter that information in exchange for advertising and marketing services. Defendant does not use the technologies in question, such as the Facebook Tracking Pixel (“Pixel”), to analyze “browsing” activities on its Website. It uses them to disclose Private Information to third parties like Facebook so Defendant can make more money through targeted advertising.

In challenging Plaintiff Jacq Nienaber’s Complaint (“Complaint” or “Compl.”) setting forth Defendant’s blatant disregard for its patients’ information, including, *inter alia*, sensitive health information and details regarding medical appointments booked through the Website, Defendant’s Motion to Dismiss (“Mot.”) ignores the actual allegations in the Complaint and the decisions of numerous courts in California and throughout the country that have sustained similar complaints at the motion to dismiss stage. *See, e.g., Doe v. Meta Platforms, Inc.*, Case No. 22-cv-

03580-WHO, 2023 WL 5837443 (N.D. Cal. Sept. 7, 2023); *Doe v. Boone Health, Inc.*, No. 22AC-CC07646, 2023 WL 4996117 (Mo. Cir. July 20, 2023); *Doe v. Regents of Univ. of California*, No. 23-CV-00598-WHO, 2023 WL 3316766 (N.D. Cal. May 8, 2023); *Stake v. Knox Community Hosp.*, No. 23OT01-0026, 2023 WL 5719594, at *3 (Ohio Com.Pl. Aug. 24, 2023); *Doe v. Bon Secours Mercy Health*, No. A2002663, 2021 WL 9939010, at *3 (Ohio Com.Pl. Nov. 22, 2021). In addition, both the U.S. Department of Health and Human Services (“HHS”) and the Federal Trade Commission (“FTC”) have concluded that tracking technologies on healthcare websites share protected health information, and therefore entities like Defendant may not disclose or share that information with third parties:

Tracking technologies on a regulated entity’s unauthenticated webpage that addresses specific symptoms or health conditions, such as pregnancy or miscarriage, or that ***permits individuals to search for doctors or schedule appointments without entering credentials*** may have access to PHI in certain circumstances. For example, tracking technologies could collect an individual’s email address and/or IP address when the individual visits a regulated entity’s webpage ***to search for available appointments with a health care provider. In this example, the regulated entity is disclosing PHI to the tracking technology vendor, and thus the HIPAA Rules apply.***^{1 2}

The Complaint clearly and sufficiently alleges that: (1) the Facebook Pixel and other tracking technologies (“Tracking Tools”) are embedded on Defendant’s Website; (2) the Tracking Tools on the Website *force* those patients’ web browsers to duplicate their communications with

¹ See *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates*, U.S. Health & Hum. Servs. <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html> (last visited November 6, 2023) (emphasis added), cited in the Complaint at ¶ 113.

² See also *FTC-HHS Joint Letter re: Use of Online Tracking Technologies*, https://www.ftc.gov/system/files/ftc_gov/pdf/FTC-OCR-Letter-Third-Party-Trackers-07-20-2023.pdf (last visited November 6, 2023). (“Impermissible disclosures of an individual’s personal health information” include “*where an individual seeks medical treatment*”; disclosure of such information without a consumer’s authorization violates FTC Act and FTC’s Health Breach Notification Rule) (emphasis added).

1 Defendant and send them to be intercepted by third parties like Facebook and Google; (3) Plaintiff
 2 used Defendant's Website to communicate Private Information, including requesting and
 3 scheduling appointments, communicating with healthcare professionals, completing medical
 4 forms, and requesting and reviewing healthcare and billing records; and, therefore (4) Defendant
 5 intercepted, recorded, and disclosed Plaintiff's confidential information to third parties. These
 6 allegations are not conclusions, hypotheticals, or speculations. They are facts. Plaintiff's claims
 7 are plausible and do not turn on what specific medical condition she had or appointment she
 8 booked. Defendant's Motion to Dismiss should be denied.

10 **II. FACTUAL BACKGROUND**

11 Defendant owns and operates the Website www.overlakehospital.org, which allows
 12 patients to, *inter alia*, search for and book appointments for medical treatment. Compl. ¶¶ 37, 75.
 13 Unbeknownst to Plaintiff and Class Members, Defendants installed Tracking Tools on the
 14 Website, including the Facebook Tracking Pixel ("Pixel") and Google Analytics, that redirected
 15 Plaintiff's and Class Members' communications and sensitive and confidential Private Information
 16 about their healthcare and medical conditions contained therein. *Id.*, ¶¶ 3, 4, 30-31, 75-80, 86-103,
 17 173, 183. The Tracking Tools surreptitiously record and force the transmission of the information
 18 Defendant's patients, including Plaintiff, provide Defendant via the Website. *See id.* ¶¶ 3, 4, 8, 15,
 19 19, 30, 31, 40, 50, 60, 68, 70, 72, 73, 80, 89, 99, 102, 103, 162, 163, 183, 245. The information
 20 sent to third parties includes Plaintiff's and Class Members' Private Information about their past,
 21 present, and future medical care, including their status as medical patients, health conditions,
 22 medical appointments, and the text or phrases they type into search bars or text boxes (such as
 23 searches for specific doctors for specific conditions). *Id.* ¶¶ 9, 79, 86, 99. The information is sent
 24 by the unsuspecting user's browser directly to those third parties and used to build profiles on the
 25
 26
 27

1 user – without authorization or consent – for purposes of retargeting and future marketing. *Id.*,
 2 ¶¶ 9, 13, 22, 38, 42, 51, 54, 129, 134-135, 216.

3 Defendant unlawfully intercepted and disclosed Plaintiff’s and Class Members’ Private
 4 Information, including not only the specific medical appointments booked and conditions entered
 5 into search boxes, but also identifying information such as the user’s IP address and Facebook ID.
 6 *Id.*, ¶¶ 7, 87-88, 101, 123-131, 246. For example, if a patient books an appointment or seeks
 7 medical services for cancer, those communications with Defendant are surreptitiously duplicated
 8 and transmitted to Facebook or Google. *Id.*, ¶¶ 75-103. Defendant subsequently uses this Private
 9 Information to retarget patients in marketing campaigns. *Id.*, ¶¶ 9, 13, 22, 38, 42, 51, 54, 129, 134-
 10 135, 216. As Defendant’s patient, Plaintiff communicated with Defendant via the Website to
 11 request and schedule appointments, communicate with healthcare professionals, complete medical
 12 forms, and request and review healthcare and billing records. *Id.*, ¶¶ 35-37. Plaintiff and Class
 13 Members did not consent to Defendant’s disclosure of their Private Information. *Id.*, ¶¶ 35, 39, 78,
 14 85, 89, 103, 108. Defendant’s conduct violates industry standards and HIPAA *Id.* ¶¶ 109-120.

17 **III. LEGAL STANDARD**

18 Under Fed. R. Civ. P. 12(b)(6), dismissal for failure to state a claim is improper where the
 19 complaint pleads “enough facts to state a claim [for] relief that is plausible on its face.” *In re*
 20 *Google RTB Consumer Priv. Litig.*, 606 F. Supp. 3d 935, 942 (N.D. Cal. 2022) (quoting *Bell Atl.*
 21 *Corp. v. Twombly*, 550 U.S. 544, 570 (2007)) (“*Google RTB IP*”). “In deciding whether the plaintiff
 22 has stated a claim upon which relief can be granted, the Court accepts the plaintiff’s allegations as
 23 true and draws all reasonable inferences in favor of the plaintiff.” *Doe v. Meta Platforms, Inc.*,
 24 2023 WL 5837443, at *2. “If the court dismisses the complaint, it ‘should grant leave to amend
 25 even if no request to amend the pleading was made, unless it determines that the pleading could
 26

not possibly be cured by the allegation of other facts.’’ *Id.* (quoting *Lopez v. Smith*, 203 F.3d 1122, 1127 (9th Cir. 2000)).

IV. ARGUMENT

A. The Complaint Alleges More Than “Tracking” Of “Public Website Browsing Activity”

Defendant’s Website is not a general information website like the cancer.net website discussed in *Smith v. Facebook*, 262 F. Supp. 3d 943 (N.D. Cal. 2017). Instead, the Website is used by *patients* as part of their continuum of medical care. This clear distinction was recognized in *Doe v. Bon Secours*, where the court observed:

Defendant first notes that its website is available to anyone, not just its patients. No doubt this is true, but *plaintiff is a patient*. Plaintiff alleges he and other patients are encouraged by defendant to use its website to obtain information about medical conditions, access medical records through the mychart portal and schedule appointments. While a non-patient may visit defendant’s website to view some of the information thereon, *in the absence of a physician-patient relationship with defendant, plaintiff and others would be unlikely to visit defendant’s website* to access their medical records or schedule appointments, actions that are allegedly disclosed to third parties.

2021 WL 9939010, at *2 (emphasis added).

Cousins v. Sharp Healthcare, 22-CV-2040-MMA (DDL), 2023 WL 4484441 (S.D. Cal. July 12, 2023), notwithstanding, courts in the Ninth Circuit and around the country have found that patient communications with a hospital website go beyond mere “browsing.” *See, e.g., Doe v. Meta Platforms*, 2023 WL 5837443, at *3 (denying motion to dismiss wiretapping and privacy claims where plaintiffs alleged that users entered their personal medical information into forms provided by hospital websites); *Doe v. Regents*, 2023 WL 3316766, at *4 (denying motion to dismiss where plaintiff alleged that hospital system intentionally incorporated Facebook Pixel on the hospital website); *Brown v. Google LLC*, No. 4:20-CV-3664-YGR, 2023 WL 5029899, at *5

(N.D. Cal. Aug. 7, 2023) (“*Brown II*”) (denying defendant’s motion for summary judgment, finding plaintiffs had standing to pursue their privacy claims although they had merely browsed publicly available websites).³ The Court should follow this overwhelming majority of cases and refuse to accept Defendant’s “browsing” defense.

B. Plaintiff Properly Pleads A Claim For Negligence.

Defendant attempts to deny owing Plaintiff a duty by mischaracterizing Plaintiff’s Complaint. The bases for Defendant’s duty lie in state statute, common law, its own policies, and federal law. In fact, the idea that a medical provider does **not** owe a duty to protect patient information strains credulity.

First, as a health care provider, Defendant owes a duty to keep health care information confidential under the Health Care Information Act (“HCIA”). Wash. Rev. Code. §§ 70.02.20, 70.02.50, and 70.02.170, *et seq.* “Health care information” is “any information... that identifies or can readily be associated with the identity of a patient and directly relates to the patient’s health care....” Wash. Rev. Code. § 70.02.20, subd. 15. *See gen. Hankins v. City of Tacoma*, No. C06-5099 FDB, 2007 WL 208419, at *2 (W.D. Wash. Jan. 24, 2007) (describing the Health Care

³ *See also, e.g., Cyr v. Orlando Health*, No. 8:23-cv-588, ECF No. 37 (M.D. Fl. July 5, 2023) (denying defendant’s motion to dismiss in full, including claims under Florida’s analogous wiretapping statute, where plaintiffs alleged hospital installed pixels on its website); *Doe v. Boone Health*, 2023 WL 4996117, at *3 (holding hospital violated patients’ privacy rights by disclosing “health information to Facebook and Google [collected] via tracking tools on its website”); *Stake v. Knox*, 2023 WL 5719594, at *3 (same). *Accord Yockey v. Salesforce, Inc.*, No. 22-cv-09067-JST, 2023 WL 5519323, at *6 (N.D. Cal. Aug. 25, 2023) (rejecting defendant’s argument that “plaintiffs had no reasonable expectation of privacy because the communications occurred over the internet”); *Javier v. Assurance IQ, LLC*, 2022 WL 1744107, at *1 (9th Cir. May 31, 2022) (plaintiff stated valid claim by alleging that he provided “demographic information and medical history” via forms filled out on insurance company website); *Google RTB II*, 606 F. Supp. 3d at 948 (denying motion to dismiss where plaintiffs alleged that “health data such as whether someone suffers from depression or eating disorders” was disclosed without their consent); *In re Pharmatrak, Inc.*, 329 F.3d 9, 12 (1st Cir. 2003) (plaintiffs stated valid wiretapping claims where “pharmaceutical companies invited users to visit their websites to learn about their drugs and to obtain rebates”).

Information Act). The information Plaintiff gave to Defendant – her healthcare provider - who in turn gave it to Facebook can be used to readily identify the Plaintiff. Compl., ¶¶ 7, 40, 50-103, 123-131, 246. Although Plaintiff does not specifically allege a claim under this statute, it nonetheless creates and defines Defendant’s duty. *See* Restatement (Second) of Torts § 286; *Clark v. TRC Env’t Corp.*, No. C09-1854-JCC, 2011 WL 3664884, at *6 (W.D. Wash. Aug. 19, 2011) (HCIA enacted because the unauthorized disclosure of health care information “may do significant harm to a patient’s interest in privacy, health care, or other interests.”).

Second, the caselaw relied on by Defendant is easily distinguishable. (*See* Def’s Mem., at 13-14.). Specifically, *In re MCG Health Data Sec. Issue Litig.*, 2:22-CV-849-RSM-DWC, 2023 WL 3057428, at *3 (W.D. Wash. Mar. 27, 2023), involved a data breach where the court held that the defendant owed no duty to the plaintiffs as a result of the “criminal acts of a third-party.” *Id.* at 3. *See also, Veridian Credit Union v. Eddie Bauer, LLC*, 295 F. Supp. 3d 1140, 1157 (W.D. Wash. 2017) (retailer not liable for criminal acts of a hacker because there was no “special relationship” between it and the plaintiff.). Defendant makes no argument that Facebook illegally accessed Defendant’s Website to steal Plaintiff’s Private Information. Instead, Defendant *itself* chose to unlawfully install tracking technologies on its Website and transmit Plaintiff’s and Class Members’ Private Information to Facebook, in violation of industry standards. Compl., ¶¶ 80-103, 116-119. Defendant is not the victim here. In the words of this Court in *Veridian*, the issue here is malfeasance, not nonfeasance. *Veridian*, 295 F. Supp. 3d at 1157.

Defendant’s own privacy policy also establishes that it owed a duty to the Plaintiff. Compl., ¶¶ 26, 28, 38, 89, 104-08, 154-165. Several courts have recently held health care providers have a duty in similar factual circumstances. *See Murphy v. Thomas Jefferson Univ. Hosps., Inc.*, No. CV

22-4674, 2023 WL 7017734, at *4 (E.D. Pa. Oct. 10, 2023); *Allen v. Novant Health, Inc.*, 1:22-CV-697, 2023 WL 5486240, at *5 (M.D.N.C. Aug. 24, 2023); *see also Rodriguez v. Mena Hospital Commission*, 2:23-CV-2002, 2023 WL 7198441, at *4 (W.D. Ark. Nov. 1, 2023) (finding, in a data breach context, “that there is a common law duty to act as a reasonably prudent health care entity to protect a patient's PII.”); *accord Buckley v. Santander Consumer USA, Inc.*, No. C17-5813 BHS, 2018 WL 1532671, at *1 (W.D. Wash. Mar. 29, 2018) (defendant owed duty to plaintiffs where it intentionally transferred private information to a third party and harm ensued.) Plaintiff has alleged that Defendant transmitted her Private Information to Facebook in violation of Defendant’s own policies and duties, and that harmed ensued. Compl., ¶¶ 35-42, 80-103.

Defendant offers no legal authority to argue that Plaintiff has failed to plead a breach, instead relying solely on mischaracterizations of the Complaint. The Complaint explains that Plaintiff used the Website for healthcare services as part of her continuum of care as Defendant’s patient and explains how the tracking technologies on the Website disclose Private Information to third parties like Facebook. Compl., ¶¶ 35-38, 75-103. Plaintiff has adequately pleaded a breach of Defendant’s duty of care.

Finally, Plaintiff has properly alleged damages. Compl., ¶¶ 33, 176, 187, 264. It is easy to understand the inherent value of Plaintiff’s Private Information here—its commercial value is the reason that it was collected by the Pixel in the first place. Several other courts considering similar allegations have concluded that the diminished value of sensitive health or personal information is sufficient to support a negligence claim. *Opris v. Sincera Reprod. Med.*, No. CV 21-3072, 2022 WL 1639417, at *8 (E.D. Pa. May 24, 2022) (“Because Plaintiffs have alleged loss of value to their PII ..., this assertion further supports that they suffered damages as a result of Sincera's

negligence”); *Flores-Mendez v. Zoosk, Inc.*, No. C 20-04929 WHA, 2021 WL 308543, at *4 (N.D. Cal. Jan. 30, 2021) (“plaintiffs adequately allege damages in the form of ... loss of privacy with respect to highly sensitive information.”) *Feins v. Goldwater Bank NA*, No. CV-22-00932-PHX-JJT, 2022 WL 17552440, at *8 (D. Ariz. Dec. 9, 2022) (similar); *Smallman v. MGM Resorts Intl.*, 638 F. Supp. 3d 1175, 1188-90 (D. Nev. 2022) (similar); *In re Marriott Intl., Inc., Customer Data Sec. Breach Litig.*, 440 F. Supp. 3d 447, 494-95 (D. Md. 2020) (similar). Courts also recognize that benefit of the bargain damages can be recovered through a negligence claim following a data breach. *See, e.g., Smallman* 638 F. Supp. 3d at 1190.⁴

Defendant’s motion to dismiss Plaintiff’s negligence claim should be denied.

C. Plaintiff Has Adequately Pled An Invasion Of Privacy Claim.

Washington recognizes a common law cause of action for invasion of privacy by intrusion upon seclusion and by public disclosure of private facts. *Armijo v. Yakima HMA, LLC*, No. 11-CV-3114-TOR, 2012 WL 2576624, *2 (E.D. Was. Jul. 3, 2012). To prevail on a claim for intrusion upon seclusion, a plaintiff must prove the defendant deliberately intruded into the plaintiff’s solitude, seclusion, or private affairs in a manner that would be highly offensive to a reasonable person. *Id.* To prevail on a claim of public disclosure of private facts, a plaintiff must prove the defendant intentionally disclosed private facts that were not of legitimate concern to the public and that the disclosure would be highly offensive to a reasonable person. *Id.*

Both standards are easily met here. Plaintiff alleges Defendant intruded upon her seclusion by deliberately planting a bug on her web browser that surreptitiously forced her to duplicate her

⁴ Defendant contends Plaintiff fails to state a negligence claim due to the economic loss rule. Mot. at 9, 13. Washington law does not recognize the economic loss doctrine. *Veridian Credit Union*, 295 F. Supp. 3d at 1150 (citing *Affiliated FM Ins. Co. v. LTK Consulting Servs., Inc.*, 243 P.3d 521, 526 (Wash. 2010)).

1 communications with Defendant and disclose them to Facebook, Google, and other third parties.
 2 Compl. ¶¶ 3, 4, 8, 15, 19, 30, 31, 40, 50, 60, 68, 70, 72, 73, 80, 89, 99, 102, 103, 162, 163, 183,
 3 245. Defendant did not have permission to access Plaintiff's computer in this way or to force the
 4 disclosure of her Private Information to third parties; in fact, Defendant explicitly stated in its
 5 Online Privacy Policy that it would not share information. *Id.*, ¶¶ 26, 28, 38, 89, 104-08, 154-165.
 6 And courts in the Ninth Circuit have repeatedly recognized that the sharing of such Private
 7 Information is highly offensive to a reasonable person. *See, e.g., In re Meta Pixel Healthcare Litig.*,
 8 No. 22-cv-03580-WHO, 2022 WL 17869218, at *14 (N.D. Cal. Dec 22, 2022) (recognizing
 9 "patient status and medical-related communications between patients and their medical providers
 10 are protected by federal law," that "health-related communications with a medical provider are
 11 almost uniquely personal," and that therefore plaintiffs had a reasonable expectation of privacy
 12 that their communications with their medical providers were confidential); *Katz-Lacabe v. Oracle*
 13 *Am., Inc.*, No. 22-cv-04792-RS, 2023 WL 2838118 at *7 (N.D. Cal. Apr. 6, 2023) (denying motion
 14 to dismiss because allegations of disclosure of "sensitive, health-related types of personal
 15 information" went well beyond "'routine commercial behavior' of collecting contact information
 16 for sending advertisements."); *Rodriguez v. Google LLC*, No. 20-cv-04688-RS, 2021 WL
 17 2026726, at *8 (N.D. Cal. May 21, 2021). *Accord Norman-Bloodsaw v. Lawrence Berkeley Lab'y*,
 18 135 F.3d 1260, 1269 (9th Cir. 1998) ("One can think of few subject areas more personal and more
 19 likely to implicate privacy interests than that of one's health or genetic make-up."). Defendant's
 20 disclosure of Plaintiff's Private Information was highly offensive.
 21
 22
 23

24 Defendant raises two arguments as to why the Plaintiff's invasion of privacy claim should
 25 be dismissed. First, Defendant argues that any invasion occurred at the hands of a third party. This
 26
 27

1 is incorrect. Defendant mistakenly relies on *Kurowski v. Rush Sys. for Health* No. 22 C 5380,
 2 2023 WL 2349606, at *9 (N.D. Ill. Mar. 3, 2023). *Kurowski* is distinguishable because it conflates
 3 the relevant theories under the tort of invasion of privacy and is contrary to caselaw from within
 4 the Ninth Circuit. In *Kurowski*, the court held no invasion of privacy occurred because third parties
 5 (not the defendant) intercepted private information and the plaintiff voluntarily gave defendant the
 6 information. 2023 WL 2349606, at *9. According to *Kurowski*'s logic, the postal service could let
 7 strangers on the street open someone's outgoing mail as long as the sender had "voluntarily" given
 8 the mail to the USPS. In any event, the Complaint here clearly sets forth that it was *Defendant*
 9 that engaged in a deliberate intrusion upon Plaintiff's seclusion by planting a bug on her web
 10 browser without consent. As the cases cited above have held, Plaintiff did not "voluntarily"
 11 provide Defendant with her Private Information under those circumstances.
 12

13
 14 Further, Plaintiff also prevails under the "publication" theory from *Guy v. Convergent*
 15 *Outsourcing, Inc.*, No. C22-1558 MJP, 2023 WL 4637318, at *2 (W.D. Wash. July 20, 2023).
 16 There, in a non-Pixel case, the court held that the plaintiffs had a viable invasion of privacy claim
 17 under Washington law where a debt-collector inadvertently disclosed private information when it
 18 was hacked in a data breach. *See gen., id.* In its reasoning, the court explained that the publication
 19 prong of an invasion of privacy claim can exist where someone fails to properly secure private
 20 information. *Id.* at *7. Defendant has taken information that is private and shown it to some of the
 21 world's largest advertising companies, who use it for targeted marketing and advertising Plaintiff
 22 did not authorize. Defendant's motion, therefore, should be denied.
 23

24 **D. Plaintiff States a Breach of Confidence Claim**

25 The Supreme Court of Washington has long "recognized a cause of action against a
 26 physician for unauthorized disclosure of confidential information." *See Berger v. Sonneland*, 144
 27

1 Wash. 2d 91, 106 (2001); *see also Smith v. Driscoll*, 94 Wash. 441, 442, 162 P. 572 (1917) (A
 2 “cause of action lies in favor of a patient against a physician for wrongfully divulging confidential
 3 communications.”). Defendant’s authorities are inapposite and should be read only to apply in the
 4 specific contexts in which they were decided. In this case, Plaintiff and the proposed Class are
 5 current and former patients of Defendant who reasonably believed that their PHI would not be
 6 disclosed to third parties. Plaintiff has stated a claim for breach of confidence.
 7

8 **E. Plaintiff Adequately States a Breach of Implied Contract Claim**

9 Plaintiff and Class Members allege that they entered an implied contract with Defendant
 10 by using Defendant’s Website, pursuant to which “Defendant agreed to safeguard and not disclose
 11 their Private Information without consent.” Compl. ¶ 189. Washington law recognizes two kinds
 12 of implied contract: those implied in law and those implied in fact. *Young v. Young*, 164 Wash. 2d
 13 477, 483-84, 191 P.3d 1258, 1262 (2008). A contract implied in fact “is an agreement depending
 14 for its existence on some act or conduct of the party sought to be charged and arising by implication
 15 from circumstances which, according to common understanding, show a mutual intention on the
 16 part of the parties to contract with each other.” *Id.* (citing *Johnson v. Nasi*, 50 Wn. 2d 87, 91, 309
 17 P.2d 380, 383 (1957)). Additionally, the services must be performed “under such circumstances
 18 that the person rendering them expected to be paid therefor, and that the recipient expected, or
 19 should have expected, to pay for them.” *Id.*
 20
 21

22 Defendant mistakenly claims that Plaintiff fails to provide factual allegations that support
 23 the existence of an implied contract. Mot. at 18. On the contrary, Plaintiff has alleged that, as
 24 Defendant’s patient, she reasonably expected her online communications with Defendant were
 25 solely between herself and Defendant and would not be transmitted or intercepted by a third party.
 26 Compl. ¶ 38. Plaintiff would not have entrusted her Private Information to Defendant in the
 27

1 absence of such an implied agreement. *Id.* ¶¶ 38, 121-122, 189-191. Defendant violated industry
2 standards, the HCIA, and its own privacy policies by sharing Plaintiff’s information without
3 consent. *Id.*, ¶¶ 39, 116-122.

4 Defendant contends that “there is no indication that any contract included alleged promises
5 to safeguard Plaintiff’s data.” Mot. at 19. However, Defendant’s Online Privacy Notice makes
6 promises to this effect. Compl. ¶ 106. Defendant made explicit representations that it would not
7 “share [Plaintiff and Class Members’] information with third parties outside of [Defendant’s]
8 organization” except in limited circumstances. *Id.* The parties had assent on this term.

9 Defendant also argues that its Notice of Privacy Practices cannot form the basis of an
10 implied contract because that notice is merely a federally mandated HIPAA notice. Mot. at 19.
11 However, several courts have found similar privacy policies instructive when discerning the terms
12 of an implied contract between patients and healthcare providers in similar cases. *Boone Health,*
13 *Inc.*, 2023 WL 4996117, at *1 (Defendant manifested an implicit promise to provide medical
14 services and institute reasonable measures to protect the confidentiality of plaintiff’s medical
15 information); *see also Doe v. Regents of Univ. of California*, 2023 WL 3316766, *1 (“It is plausible
16 that the parties entered into an implied contract by their actions. The agreed upon terms of this
17 implied contract are those spelled out in the Notice of Privacy and Privacy Statement, providing
18 assurances.”).

19 Defendant’s final claim posits that “the damages Plaintiff seeks are not recoverable in
20 contract.” Mot. at 19. This contention ignores a “growing trend across courts that have considered
21 this issue is to recognize the lost property value of [personal] information.” *In re Marriott Int’l,*
22 *Inc., Customer Data Sec. Breach Litig.*, 440 F. Supp. 3d 447, 460 (D. Md. 2020); *In re Experian*
23
24
25
26
27

1 *Data Breach Litig.*, No. SACV-15-1592 AG (DFMx), 2016 WL 7973595 (C.D. Cal. Dec. 29,
 2 2016) (“[A] growing number of federal courts have now recognized Loss of Value of PII as a
 3 viable damages theory”); *In re Facebook Privacy Litig.*, 572 F. App’x 494 (9th Cir. 2014); *Klein*
 4 *v. Facebook, Inc.*, 580 F. Supp. 3d 743, 804 (N.D. Cal. 2022) (“[T]here is ample support for
 5 Consumers’ argument that lost information and attention has material value.”); *Smallman*, 638 F.
 6 Supp. 3d at 1190 (collecting cases and noting that “these pleading requirements, that Plaintiffs
 7 must establish both the existence of a market for their PII and an impairment of their ability to
 8 participate in that market, is not supported by Ninth Circuit precedent and other district courts in
 9 this Circuit have rejected them.”). *See also In re Mednax Servs., Inc., Customer Data Sec. Breach*
 10 *Litig.*, 603 F. Supp. 3d 1183, 1204 (S.D. Fla. 2022) (“plaintiffs need not reduce their PHI or PII to
 11 terms of dollars and cents in some fictitious marketplace where they offer such information for
 12 sale to the highest bidder.”)(citing *Klein*, 580 F. Supp. at 802-04). Plaintiff has stated a claim for
 13 breach of implied contract.
 14
 15

16 **F. Plaintiff Adequately States an Unjust Enrichment Claim**

17 Unjust enrichment “occurs when one retains money or benefits which in justice and equity
 18 belong to another.” *Bailie Commc’ns, Ltd. v. Trend Bus. Sys., Inc.*, 810 P.2d 12, 18 (Wash. App.
 19 1991). To state a claim for unjust enrichment, Plaintiff must show that: 1) Plaintiff conferred a
 20 benefit upon Defendant, 2) at Plaintiff’s expense, and 3) the circumstances make it unjust for
 21 Defendant to retain the benefit without payment. *Young v. Young*, 191 P.3d 1258, 1262 (Wash.
 22 App. 2008).
 23

24 Defendant erroneously asserts that Plaintiff fails to plead facts showing these elements.
 25 Mot. at 20. Plaintiff satisfies the first element by alleging that she conferred a benefit on Defendant
 26 by providing it with her Private Information in exchange for medical services offered by
 27

1 Defendant. Compl. ¶ 38, 121-122, 197. Defendant received clear economic, intangible, and
 2 business benefits from its receipt of Plaintiff's Private Information, and used the valuable data
 3 obtained via the Pixel and other Tracking Tools for marketing purposes in an effort to bolster its
 4 revenues. *Id.*, ¶¶ 13, 132-135, 173.

5
 6 Second, Plaintiff suffered a concrete detriment due to the unauthorized disclosure of her
 7 Private Information without her consent. Compl. ¶¶ 40, 78, 85, 89, 187. Because of Defendant's
 8 use of the Pixel, Plaintiff and Class Members suffered from: "(i) invasion of privacy, (ii) lost time
 9 and opportunity costs associated with attempting to mitigate the actual consequences of the Pixel,
 10 (iii) loss of benefit of the bargain, (iv) diminution of value of the Private Information, (v) statutory
 11 damages, and (vi) the continued and ongoing risk to their Private Information." *Id.* ¶33.

12
 13 Finally, the circumstances in this case make it unjust for Defendant to retain the benefit
 14 conferred. Plaintiff has alleged that Defendant benefitted twofold from Plaintiff's provision of her
 15 Private Information. First, Defendant has received financial compensation from Plaintiff as a
 16 result of providing medical services that she would not have paid for had she known Defendant
 17 was sharing her Private Information. *Id.* ¶ 38, 191, 193. Second, Defendant benefitted from the
 18 disclosure of Plaintiffs' Private Information for marketing and retargeting. *Id.* ¶ 13, 42, 132-135,
 19 173. Plaintiff specifically has alleged that Defendant's use of the Pixel reduced the "cost of
 20 advertising and retargeting." *Id.* ¶ 135. Defendant accrued these benefits at the direct and unwitting
 21 expense of Plaintiff and Class Members. Allowing Defendant to retain these benefits without
 22 compensation to Plaintiff and Class Members would present an injustice of the highest order.

23
 24 Similar claims for unjust enrichment in the context of disclosure of patients' medical
 25 information through use of the Pixel have been upheld in *Doe v. Meta Platforms, Inc.*, 2023 WL
 26

5837443, at *13 and *Doe v. Boone Health*, Case No. 22A-CC07646, 2023 WL 4996117 at p. 7 (Mo. Cir. July 20, 2023) (stating “Plaintiff has plausibly pled a claim for unjust enrichment” and reciting identical elements).⁵

G. Plaintiff’s Claims Under the Electronic Communications Privacy Act (“ECPA”) (Counts VI-VIII) are Well Pled.

With commendable legerdemain, Defendant attempts to evade liability for the exact conduct the ECPA was written to protect against. Defendant argues that “recording” is the same as “transmitting,” that Plaintiff merely alleged a claim of “aiding and abetting” a third party in violating the ECPA, that no actual contents were allegedly disclosed, and that despite providing a service allowing patients to communicate electronically with their healthcare providers, they are not subject to the ECPA. Mot. at 20-27. These arguments are as bold as they are flimsy.

1. Plaintiff Appropriately Invokes the Tortious or Criminal Conduct Exception to the One-Party Consent Rule.

Plaintiff alleges that Defendant deployed Tracking Tools, such as the Pixel and Conversions API, on its website, patient portal, and server. *See* Compl. ¶¶ 3, 4, 30, 31, 80, 103, 173, 183. Plaintiff further alleges that these Tracking Tools surreptitiously record the information the Defendant’s patients, including Plaintiff, provide Defendant via the website or patient portal. *See id.* ¶¶ 3, 4, 8, 15, 19, 30, 31, 40, 50, 60, 68, 70, 72, 73, 80, 89, 99, 102, 103, 162, 163, 183, 245. In addition to recording this information, these Tracking Tools transmit the recorded information to third parties, such as Facebook and Google. *See id.* Finally, Plaintiff alleges that

⁵ *Heeger v. Facebook, Inc.*, 509 F. Supp. 3d 1182, 1191 (N.D. Cal. 2020), involved an examination of California’s law concerning unjust enrichment as part of a federal standing analysis and is inapposite.

1 the purpose behind Defendant's use of these Tracking Tools is to drive marketing for Defendant
2 and increase its profitability. *See id.* ¶¶ 13, 51, 72, 132, 216.

3 Under the ECPA, where a private electronic communication is intercepted for the purpose
4 of committing a crime or tortious act, a defendant may be liable even if it is a party to the
5 communication. 18 U.S.C. § 2511(2)(d). As Defendant points out, that crime or tortious act must
6 generally be "independent or the intentional act of recording." Mot. at 22, quoting *In re Google*
7 *Cookie Placement Consumer Priv. Litig.*, 806 F.3d 125, 145 (3rd Cir. 2015). Defendant seems to
8 rely on the Court interpreting the act of *recording* Plaintiff's and Class Members' communications
9 as the same act as *transmitting* those communications to third parties in violation of Defendant's
10 duties of care and confidentiality. But these acts are distinct and are clearly pleaded as such.

11 Defendant surreptitiously recorded Plaintiff's and Class Members' communications with
12 their healthcare professionals, then transmitted those recorded communications to third parties for
13 the purpose of increasing Defendant's profitability. This purpose violates numerous state and
14 federal laws, including HIPAA and the Washington Consumer Protection Act, among others. *See*
15 Compl. ¶¶ 101, 109-115, 270, 273, 274. Essentially, Defendant unlawfully planted a bug on
16 Plaintiff's web browsers and forced her to transmit information to Facebook so Defendant could
17 obtain discounted advertising and marketing services as described in the Complaint. Plaintiff
18 would not have disclosed her Private Information to Defendant had she known Defendant would
19 turn around and disclose it to Facebook.

20
21
22
23 **2. Plaintiff's Allegations Clearly and Adequately Set Forth Her**
24 **Claims Under the ECPA.**

25 Defendant asserts that Plaintiff merely alleges facts that would support the "aiding and
26 abetting" of an interception of Plaintiff's communications. Mot. at 23. Defendant also argues that,

1 even if Plaintiff argues that Defendant is directly culpable for its conduct, Plaintiff still fails to
 2 plead that adequate contents of her communications were intercepted.⁶ *Id.* at 24-25. These
 3 arguments again either misread or misconstrue Plaintiff's allegations and are, once corrected,
 4 unpersuasive.

5 First, Plaintiff does not allege that Defendant "aided and abetted" anyone in the
 6 commission of an ECPA violation. Rather, Plaintiff alleges that Defendant intentionally used
 7 Tracking Tools designed by third parties, such as Facebook and Google, and that Defendant is
 8 liable for its choice to configure and deploy these Tracking Tools on its website and patient portal
 9 in commission of tortious and criminal conduct. Plaintiff alleges clearly that Defendant is the
 10 principal party to the violation of the ECPA, so no secondary liability theory is required.

11 Defendant incorrectly contends that Plaintiff fails to allege that the contents of her private
 12 communications were intercepted. Plaintiff alleges that information such as her IP address, Pixel
 13 ID, and Facebook ID were all intercepted by the Tracking Tools and transmitted to third parties
 14 for the purpose of deanonymizing other intercepted information. That other intercepted
 15 information included: Plaintiff's requests for specific medical appointments and the purposes for
 16 those appointments, actual written communications between Plaintiff and her healthcare
 17 professionals, the information Plaintiff entered onto completed medical forms, and
 18 communications related to Plaintiff's review of her medical records and bills. *See, e.g.,* Compl.
 19 ¶ 37.

20
 21
 22
 23
 24
 25 ⁶ Defendant also alludes to the argument that no device was used to intercept the communications,
 26 "only software." Setting aside that this argument is unexplored and unsupported, software is a
 27 "device" for wiretapping purposes. *See Doe v. Meta Platforms, Inc.*, 2023 WL 5837443 (citing
In re Carrier IQ, Inc., 78 F. Supp. 3d 1051 (N.D. Cal. 2015)).

Moreover, though Defendant argues that a general URL should not be considered contents of a communication, Defendant's Tracking Tools convey *descriptive* URLs, which are distinct. Mot. at 24. As illustrated in the Complaint, at paragraphs 94-98, the URL transmitted by Defendant's Pixel isn't merely "www.overlakehospital.org," but rather a much longer chain of text including information regarding specific interactions a person has with Defendant's website or patient portal, including searches for specific doctors or medical conditions. These specifics are unique to descriptive URLs and are not the kind of URLs analyzed by the court in either *Facebook Internet Tracking Litig.*, 140 F. Supp. 3d 922, 935 (N.D. Cal. 2015), or *In re Zynga Priv. Litig.*, 750 F.3d 1098, 1106–07 (9th Cir. 2014), as referenced by Defendant. The generic URL in *Zynga* is not analogous to the URL in this case, which would not only disclose the visit to the page, but would *also* disclose the inputs on the webpage, including whether the visitor checked a calendar, scheduled a visit, entered any information, or visited the page from a browser where they had used their Facebook account. The factual distinction between a basic URL and a descriptive URL is critical. *See, e.g., In re Meta Pixel Healthcare Litig.*, 2022 WL 17869218, at *11 ("the log-in buttons" and "descriptive URLs ... are 'contents' within the meaning of the statute."); *Doe v. Meta Platforms, Inc.*, 2023 WL 5837443, at *3 ("a URL disclosing a 'search term or similar communication made by the user' 'could constitute a communication' under the statute"); *Google RTB II*, 606 F. Supp. 3d at 949 (N.D. Cal. 2022) (finding that categories of the website, categories that describe the current section of the website, and referrer URL that caused navigation to the current page constituted "content").

1 **3. Defendant Provides an Electronic Communication Service and**
 2 **is Subject to the ECPA and the Stored Communication Act**
 3 **(“SCA”).**

4 Defendant next asserts that it is immune from the ECPA because its Website is not an
 5 “electronic communications service.” Mot. at 25-27. The ECPA, however, defines “electronic
 6 communication service” as “any service which provides the users thereof the ability to send or
 7 receive wire or electronic communications.” 18 U.S.C. § 2510(15). Courts construe this language
 8 broadly to encompass entities that provide two-way messaging platforms. *See e.g., United States*
 9 *v. Mullins*, 992 F.2d 1472, 1474 (9th Cir. 1993) (Airline whose reservation system allowed
 10 consumers to book flights and modify reservations is an electronic communication service); *In re*
 11 *United States for an Ord. Pursuant to 18 U.S.C. §2703(d)*, No. MC 17-2682 (BAH), 2018 WL
 12 1521772, at *5 (D.D.C. Mar. 8, 2018) (defining cruise line as an electronic communication service
 13 because it provided customers with a system to send and receive messages “regardless of whether
 14 its primary business function is the provision of ECS.”). Defendant’s Website and patient portal
 15 provide its patients exactly that—the ability to send to and receive communications from their
 16 healthcare providers. *See, e.g., Compl.*, ¶¶ 3, 23, 31, 37, 79, 83, 90, 224. Indeed, this is the primary
 17 purpose of Defendant’s Website.

18
 19 Defendant’s systems are thus not akin to an online retailer, where the communication is
 20 incidental to the purchase of goods or services. *See e.g., Wesch v. Yodlee, Inc.*, No. 20-CV-05991-
 21 SK, 2021 WL 6206644, at *3 (N.D. Cal. July 19, 2021) (“Plaintiffs do not and cannot allege that
 22 they use Yodlee to send their financial institutions a message. Therefore, Yodlee is more akin to
 23 Amazon than a service which allows parties to send and receive messages to each other.”). Rather,
 24 Defendant encourages its patients to use a two-way communication platform and encourages
 25 patients to use it as a substitute for in-person communications. *See, e.g., Compl.*, ¶¶ 25, 174. This
 26
 27

1 is materially different from a consumer placing an item in their shopping cart or navigating the
 2 check-out process, as Defendant’s platform was designed to facilitate communications and not
 3 commerce. *See Ehling v. Monmouth-Ocean Hosp. Serv. Corp.*, 961 F. Supp. 2d 659, 667 (D. N.J.
 4 2013) (Facebook is an ECS because it provides a private communications platform via messages
 5 and Facebook wall posts). Accordingly, Defendant’s Website is an electronic communication
 6 service and is subject to the requirements of the ECPA.
 7

8 The cases Defendant relies on are also misapplied. For example, the court in *Kurowski* did
 9 not emphatically state that all hospital networks and healthcare providers “cannot plausibly be
 10 considered an electronic communications service provider within the meaning of the Act.” 2023
 11 WL 2349606. Rather, *Kurowski* adjudicated only that the third-party provided web portal could
 12 not be attributed to the defendant in that case. This issue is absent here, where Defendant’s Website
 13 and first party patient portal themselves, not just a third-party portal, contained the tracking Pixel
 14 at issue. *See e.g.*, Compl., ¶¶ 3, 4, 30, 31, 80, 103, 173, 183. Indeed, much of Defendant’s authority
 15 is distinguishable because it discusses third-party culpability not at issue here. The bad actor in
 16 this case is Defendant itself; there is no scapegoat. Plaintiff’s claims under the Federal Wiretap
 17 Act and Stored Communications Act are adequately and properly pleaded.
 18

19 **H. Plaintiff Adequately Alleges a Claim under the CFAA for Defendant’s**
 20 **Unauthorized Access of Plaintiff’s Computer under False Pretenses**

21 A defendant violates the CFAA when it “intentionally accesses a computer without
 22 authorization or *exceeds authorized access*, and thereby obtains ... information from any protected
 23 computer.” 18 U.S.C. §§ 1030(a)(2), 1030(a)(2)(C) (emphasis added). Plaintiff alleges that
 24 Defendant exceeded its authorized access by forcing Plaintiff’s and Class Members’ web browsers
 25 to copy their private communications and transmit that information to Facebook. Compl., ¶¶ 6-7,
 26

1 30-34, 74-103. These allegations are sufficient to establish a violation of the CFAA and the
2 requisite intent. *See* 18 U.S.C. §§ 1030(a)(2), 1030(a)(2)(C).

3 Where a defendant accesses information from a protected computer under false pretenses
4 – such as here, where a hidden tracking device was employed by Defendant to copy and transmit
5 information from a protected computer – courts have held the access is unauthorized. *See, e.g.,*
6 *America Online, Inc. v. LCGM, Inc.*, 46 F.Supp.2d 444 (E.D. Va., 1998) (actions that violate the
7 terms of service established by the accessing party are unauthorized).

9 Defendant cites *Van Buren v. United States*, 141 S.Ct. 1648 (2021), to claim that “exceeds
10 authorized access” refers merely to “access restrictions” not “use restrictions.” Put differently,
11 Defendant argues that because the information it misappropriated was communicated to it, it was
12 entitled to use that information in whatever manner it pleased. Mot. at 27-28. Defendant’s reliance
13 on *Van Buren* is misplaced. In *Van Buren*, the individual in question had authorized access to the
14 computer in question, but that authorization was legitimately obtained, although the authorized
15 user later accessed the same device without authorization. 141 S.Ct. at 1653. Here, Defendant
16 obtained authorization, but under false pretenses (i.e., without disclosure of its surreptitious use of
17 Tracking Tools), then used the Tracking Tools to record and transmit Private Information and
18 communications without Plaintiff’s knowledge or consent. Defendant’s entire access to the
19 information contained in Plaintiff’s communications and devices was illegitimate, much like in
20 *America Online Inc.*, where defendant’s actions violated the terms of service and were found to be
21 unauthorized. 46 F.Supp.2d 444, 451.

24 The CFAA does additionally require a plaintiff to allege at least one of the necessary factors
25 under 18 U.S.C. § 1030(c)(4)(A)(i) to properly assert a claim. Plaintiff satisfies this requirement
26

by alleging loss and damage in ¶¶ 264-65. The CFAA includes broad definitions for both “loss”⁷ and “damage,”⁸ and courts have held that impairment to the integrity of data or personal information qualifies as damage for the purposes of a CFAA claim. *See, e.g., I.M.S. Inquiry Mgmt. Sys., Ltd. v. Berkshire Info. Sys., Inc.*, 307 F. Supp. 2d 521, 525 (S.D.N.Y. 2004) (finding sufficient allegations of CFAA damages despite lack of allegations of physical damage to data); *In re Toys R Us, Inc., Privacy Litig.*, No. 00-cv-2746, 2001 WL 34517252, at *10-11 (N.D. Cal. Oct. 9, 2001). Plaintiff has sufficiently alleged facts to support a claim under the CFAA.

I. Plaintiff Has Sufficiently Pled A Claim Under The Washington Consumer Protection Act.

Washington's Consumer Protection Act (“CPA”) prohibits “[u]nfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce.” Wash. Rev. Cod. § 19.86.020. “To prevail in a private CPA claim, the plaintiff must prove (1) an unfair or deceptive act or practice, (2) occurring in trade or commerce, (3) affecting the public interest, (4) injury to a person's business or property, and (5) causation.” *Panag v. Farmers Ins. Co. of Wash.*, 204 P.3d 885, 889 (Wash. 2009). Either an unfair or a deceptive act can be the basis for a CPA claim. *Klem v. Wash. Mut. Bank*, 295 P.3d 1179, 1187 (Wash. 2013). “An unfair act is established by evidence that it (1) causes or is likely to cause substantial injury, which (2) consumers cannot avoid, and (3) is not ‘outweighed by countervailing benefits.’” *Veridian Credit*

⁷ The term “loss” is defined in the statute as “any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service.” 18 U.S.C. §§ 1030(c)(4)(A)(i)(I), 1030(g), and 1030(e)(11).

⁸ The term “damage” is defined as “any impairment to the integrity or availability of data, a program, a system, or information.” 18 U.S.C. §§ 1030(c)(4)(A)(i)(I), 1030(g), and 1030(e)(8).

1 *Union*, 295 F. Supp. 3d at 1161 (citations omitted). The CPA “shall be liberally construed [so] that
2 its beneficial purposes may be served.” *Id.* (citations omitted).

3 Plaintiff alleges each of the required elements under the CPA. Defendant’s conduct in using
4 hidden Tracking Tools was unfair and deceptive because it violated HIPAA, industry standards,
5 and Defendant’s own privacy policies. Compl., ¶¶ 33, 176, 187(g), 264, 267-276. And the growing
6 trend across the Ninth Circuit is to recognize that personal information is not only property as
7 defined by state consumer protection statutes, but that its value is diminished by its compromise.
8 *Brown v. Google, LLC*, 2021 WL 6064009, at *15 (N.D. Cal. Dec. 22, 2021) (“*Brown I*”) (noting
9 that the unauthorized disclosure of personal information impugns a property interest and thus
10 confers standing under the UCL); *Klein*, 580 F. Supp. 3d at 804 (“[T]here is ample support for
11 Consumers’ argument that lost information and attention has material value.”); *Rex v. Chase Home*
12 *Fin. LLC*, 905 F. Supp. 2d 1111, 1145 (C.D. Cal. 2012) (noting that UCL standing does not require
13 a tangible monetary expenditure). *See also Mednax*, 603 F. Supp. 3d at 1204 (“plaintiffs need not
14 reduce their PHI or PII to terms of dollars and cents in some fictitious marketplace where they
15 offer such information for sale to the highest bidder.”) (citing *Klein*, 580 F. Supp. 3d at 802-04);
16 *Smallman*, 638 F. Supp. 3d at 1190 (collecting cases and noting that “these pleading requirements,
17 that Plaintiffs must establish both the existence of a market for their PII and an impairment of their
18 ability to participate in that market, is not supported by Ninth Circuit precedent and other district
19 courts in this Circuit have rejected them.”).

20 Defendant makes an irrelevant argument that Plaintiff is not a participant in the market —
21 which has nothing to do with the CPA – and that Plaintiff has not suffered an injury. Similar
22 arguments were rejected in *Veridian* and *Guy*. *Veridian Credit Union*, 295 F. Supp. 3d at 1161-63;
23
24
25
26
27

1 *Guy*, 2023 WL 4637318, at *8. In the context of data breaches, the cases found that the plaintiffs
 2 pled a sufficient claim under the CPA where the defendants failed to adequately protect personal
 3 information that was less sensitive than the information at issue in this lawsuit. *Id.* Further, in
 4 *Veridian* and *Guy*, the courts held that the diminution of the plaintiffs' private information or
 5 violation of the CPA itself constituted an injury under the CPA. *Id.*

6
 7 Here, the Plaintiff's allegations plead a sufficient claim under the CPA and ensuing
 8 damages that have been recognized under applicable Washington legal authority. Defendant's
 9 motion should therefore be denied.

10 **V. CONCLUSION**

11 For the reasons set forth herein, Defendant Overlake Hospital Medical Center's Motion to
 12 Dismiss should be denied.

13
 14 Respectfully submitted,

15 Dated: November 6, 2023

/s/ Andrew A. Lemmon

16 Andrew A. Lemmon (#53034)

**MILBERG COLEMAN BRYSON PHILLIPS
 17 GROSSMAN PLLC**

18 16212 Reitan Road NE

Bainbridge Island, WA 98110

19 Telephone: (985) 783-6789

alemmon@milberg.com

20 Gary M. Klinger*

21 Alexandra H. Honeycutt*

**MILBERG COLEMAN BRYSON PHILLIPS
 22 GROSSMAN PLLC**

23 227 W. Monroe Street, Suite 2100

Chicago, IL 60606

24 Telephone: (866) 252-0878

25 gklinger@milberg.com

1 Terence R. Coates*
Jonathan T. Deters*
2 **MARKOVITS, STOCK & DEMARCO, LLC**
119 E. Court Street, Suite 530
3 Cincinnati, OH 4502
Telephone: (513) 651-3700
4 Facsimile: (513) 665-0219

5
6 Bryan L. Bleichner
Philip J. Krzeski
7 **CHESTNUT CAMBRONNE PA**
100 Washington Avenue South, Suite 1700
8 Minneapolis, MN 55401
Telephone: (612) 339-7900
9 Facsimile: (612) 336-2540
10 bbleichner@chestnutcambronne.com
pkzeski@chestnutcambronne.com

11 Joseph M. Lyon*
12 **THE LYON LAW FIRM**
2754 Erie Avenue
13 Cincinnati, OH 45208
Telephone: (513) 381-2333
14 Facsimile: (513) 766-9011
15 jlyon@thelyonfirm.com

16 *Attorneys for Plaintiff and the Putative Class*

17 *I certify that this document contains 7,753 words, in*
18 *compliance with the Local Civil Rules.*